URPS médecins libéraux Auvergne Rhône Alpes

Cybersécurité

Le Guide des bonnes pratiques de l'informatique édité notamment par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) présente **12 recommandations** qui constituent un corpus incontournable.

1. **Choisir des mots de passe composés de chiffres & de lettres (dont des majuscules) et penser à les changer régulièrement. Varier les mots de passe.**
2. **Mettre régulièrement à jour ses logiciels de sécurité (antivirus et pare-feu).**
3. **Contrôler les accès des utilisateurs et prestataires.**
4. **Effectuer des sauvegardes régulières, les vérifier et les stocker sur disque dur externe déposé à l'extérieur du cabinet.**
5. **Sécuriser l'accès Wi-Fi de votre cabinet (voire le désactiver - Est-il vraiment nécessaire ?).**
6. **Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur.**
7. **Protéger ses données lors de ses déplacements. Être extrêmement vigilant lors de l'utilisation d'un Wi-Fi public.**
8. **Être précautionneux lors de l'utilisation de sa messagerie : déposer les pièces jointes sur le disque dur avant de les ouvrir (elles seront ainsi analysées par l'antivirus), vérifier l'adresse de l'expéditeur…**
9. **Télécharger ses programmes sur les sites officiels des éditeurs.**
10. **Être vigilant lors d'un paiement sur Internet : est-ce un site sécurisé ? Le https et un cadenas doivent apparaître dans l'adresse du site. N'utiliser que les sites bancaires pour faire vos achats.**
11. **Séparer les usages personnels des usages professionnels. Rédiger une charte informatique à faire signer par les collaborateurs et employés.**
12. **Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.**

RGPD

Règlement Général sur la Protection des Données personnelles

URPS médecins libéraux Auvergne Rhône Alpes

Les six points européens

- Redéfinition du consentement
- Des données supprimées lorsqu'elles deviennent obsolètes
- Minimisation et restriction du traitement des données
- Intégrité des données
- Confidentialité
- Risques encourus en cas de non-respect du Règlement

Les obligations des médecins

- **Le dossier médical** : Respecter les obligations de fond, mettre en place un **registre** (exemple : **https://bit.ly/2LrGmJS**), sécuriser l'accès aux données, veiller à la durée de conservation des données...
- **La prise de rendez-vous** : Mêmes obligations que pour les dossiers (limitation du recueil d'informations, tenue à jour des traitements).
- **La messagerie électronique** : Utiliser les messageries sécurisées lors des échanges d'informations avec les professionnels de santé.
- **Les smartphones et tablettes** : Veiller à ce que l'accès aux applications médicales soit sécurisé, éviter de stocker des données sur ces outils.
- **La télémédecine** : Toute séance de télé-consultation doit passer par des outils sécurisés.
- **Les objets connectés** : S'interroger sur le cryptage, l'hébergement et la sécurisation de ses accès, le traitement des données...

Pour en savoir plus, consultez le site de l'URPS Médecins
[CYBERSÉCURITÉ] ET [RGPD] https://bit.ly/2OZ9NpY

Pour plus d'informations, consultez ce site : www.12h15.fr/se-proteger

urps@urps-med-aura.fr

URPS Médecins Libéraux Auvergne-Rhône-Alpes
20, rue Barrier 69006 LYON ~ 04 72 74 02 75
24, allée Évariste Galois 63170 AUBIÈRE ~ 04 73 27 77 44